NIILM University International Journal of Applied and Behavioural Sciences (IJABS)

ISSN: 3048-9083 2024, Vol.01, Issue 01

POLYNOMIALS BELONGING TO GALOIS GROUP AND IT'S SOLVABILITY PROBLEMS

Pritee[1], and Jakhar, Manjeet Singh[2]

Research Scholar[1], Associate Professor[2]

[1&2]Department of Mathematics, NIILM University, Kaithal (Haryana) India

DOI: https://doi.org/10.70388/ijabs24706

Received on Jun 10, 2024

Accepted on Jun 30, 2024

Published on July 30, 2024

ABSTRACT

The fundamental focus of field theory is the investigation of algebraic extensions of fields, while the investigation of the structures of algebra known as groups is what is covered in group theory. The Galois theory is a branch of algebraic mathematics that studies the connection between these two other subfields of the subject. Everest Galois, a French mathematician, is credited with being the first person to have the idea for it, which he had around the turn of the 19th century. Galois theory offers a complete view of the solutions that may be found for polynomial equations and investigates the symmetries that are already present in these solutions. This view can be used to solve polynomial problems. This mathematical concept was given its name in honor of the French mathematician Roger Galois. A connection between field extensions and the subgroups of the Galois group that is associated with the extension is forged as a direct result of the aforementioned fact, which links the extension. The Galois group helps in the categorization of the solutions to polynomial equations and is responsible for capturing the symmetries of the field extension. Additionally, it helps with the organization of the solutions into categories.

Keywords: Galois, Group, Orthogonal, Polynomials

INTRODUCTION

Galois group: solvability of polynomial problems.

In algebra and number theory, one of the most important concepts to understand is called the Galois group of a polynomial. It is named after the mathematician Galois and refers to the symmetries as well as the structure of the roots of the polynomial that is being examined. It is feasible to think of the Galois group of a given polynomial as the "family" of that particular polynomial. This is because the Galois group is a group of groups. It has substantial consequences in a number of different areas of mathematics, which may be split down even further into subfields, in addition to giving valuable information on the solvability of polynomial problems.

If you are thinking about polynomials with a degree of five or more, you will run into one of the most difficult challenges associated with the Galois group. The Abel-Ruffini theorem, which was formulated in the 19th century, asserts that there is no universal algebraic solution for polynomials of degree five or higher that integrate radicals (expressions that entail roots). This theorem claims that there is no universal algebraic solution for polynomials of degree five or higher. This assertion was stated in relation to the fact that there is no such thing as a universal solution to an algebraic problem. To express the roots of such polynomials using a constrained number of additions, subtractions, multiplications, divisions, or root extractions is a challenging task. This is because such polynomials have an unlimited number of variables, which explains why this is the case. According to this theorem, the Galois groups of irreducible polynomials of degree five or higher must have components that cannot be expressed using radicals. This conclusion is drawn from the fact that the Galois groups exist. This is due to the fact that this particular theorem implies that irreducible polynomials cannot be simplified into more straightforward expressions. This is owing to the fact that this specific theorem claims that irreducible polynomials of degree five or higher cannot be reduced. The reason for this may be found in the previous sentence. It is usual practice to refer to these components as "transcendental" or "non-solvable" components. Both of these terms accurately describe their nature. It is hard to properly explain or describe the structure of these groups by referring just to radicals since the Galois groups that are associated with these polynomials have a structure that is both complicated and changeable because of this. The study of Galois groups has led to a number of significant theorems as well as discoveries in the field of number theory. The results of the inquiry are presented in this section. The theorem of Galois is one of the most

important discoveries ever made because it establishes a relationship between certain subgroups of the Galois group of a polynomial and intermediate fields of the splitting field of that polynomial. This is one of the most significant finds ever made. Galois is credited as being the one who first proposed this specific theorem. The capacity to solve the equations and the research of field extensions are both significantly affected by the repercussions that this finding has brought to light.

OBJECTIVE OF THE STUDY

1. To study Possibility of construction using regular polygons.
2. To study The Most Important Factor in Dividing the Terms of An Arithmetic Progression.

History Of Galois Theory

The study of field expansions, which may be thought of as mathematical frameworks that broaden the number field, is the primary emphasis of the area of mathematics that is known as Galois theory. This topic is a subfield of number theory, which is an overarching field that contains several subfields. It is believed that Évariste Galois, a French mathematician who was active throughout the 19th century and resided in France, was the first person to come up with the concept. Galois theory offers a comprehensive explanation of the connection that holds between the answers to a polynomial equation and the structure of the field extension that is connected to that equation. This explanation is provided in the context of providing an answer to an equation. This comprehension is presented within the framework of an extended field that is associated with the equation.

Galois was interested in finding a solution to an issue in mathematics at the time that had been around for a very long period. This issue, which was referred to as the solvability of equations by radicals, was one that Galois was attempting to resolve by finding a solution. Galois was particularly interested in finding a solution to this problem so that it might be resolved once and for all. To assess whether or not it was feasible to solve an arbitrary polynomial equation of degree five or higher by making use of a combination of the mathematical operations of addition, subtraction, multiplication, division, and taking roots, the goal of this task was to determine whether or not it was possible to do so. Galois tackled the issue by first investigating the symmetry connections and then the permutation possibilities that included the roots of polynomial equations.

Galois Theory

The fundamental focus of field theory is the investigation of algebraic extensions of fields, while the investigation of the structures of algebra known as groups is what is covered in group theory. The Galois theory is a branch of algebraic mathematics that studies the connection between these two other subfields of the subject. Everest Galois, a French mathematician, is credited with being the first person to have the idea for it, which he had around the turn of the 19th century. Galois theory offers a complete view of the solutions that may be found for polynomial equations and investigates the symmetries that are already present in these solutions. This view can be used to solve polynomial problems. This mathematical concept was given its name in honor of the French mathematician Roger Galois. A connection between field extensions and the subgroups of the Galois group that is associated with the extension is forged as a direct result of the aforementioned fact, which links the extension. The Galois group helps in the categorization of the solutions to polynomial equations and is responsible for capturing the symmetries of the field extension. Additionally, it helps with the organization of the solutions into categories.

Possibility of construction using regular polygons

In case you need a refresher, the explanation of how the phi function of Euler works may be found in section 1. φ(n). We will demonstrate that a regular n-gon can be constructed if and only if (n) is a power of 2, and we will do so by demonstrating that a regular n-gon can be constructed if and only if the central angles 2/n can be constructed, and we will demonstrate that this is possible if and only if a regular n-gon can be constructed cos(2π/n) is a number that can be constructed.

$$\text{Let } \omega = e^{2\pi i/n} = cos(2\pi/n) + isin(2\pi/n)$$

Become the nth primitive root of the unity. Then $cos(2\pi/n) = \frac{1}{2}(\omega + \omega^{-1})$, since $\omega^{-1} = cos(2\pi/n) - isin(2\pi/n)$. Thus $cos(2\pi/n) \in \mathbb{Q}(\omega)$.

However $\cos(2\pi/n) \in \mathbb{R}$ and $\omega \notin \mathbb{R}$, so $\mathbb{Q}(\omega) \neq \mathbb{Q}(\cos(2\pi/n))$. But ω is a root of $x^2 - 2cos(2\pi/n)x + 1$, and so $[\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/n))] = 2$ Therefore if

$\cos(2\pi/n)$ is constructible, then $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$ is a power of 2. Hence, $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$ is also a power of 2.

Conversely, suppose that φ(n) is a power of 2. The field Q(ω) is a Galois extension of Q with Abelian Galois group If $H = Gal(\mathbb{Q}(\omega) : \mathbb{Q}(\cos(2\pi/n)))$ by the theory of finite Abelian groups there is a chain of subgroups

With $|H_{i-1} - H_i| = 2$. If $L_i = \mathcal{F}(H_i)$, then $[L_i : L_{i+1}] = 2$, thus $L_i = L_{i+1}(\sqrt{u_i})$ for some ui. Since $L_i \subseteq \mathbb{Q}(\cos(2\pi/n)) \subseteq \mathbb{R}$, Every one of the ui ≥0. We can see that anything in is a number that can be produced since the square root of a number that can be constructed is likewise a number that can be constructed. $\mathbb{Q}(\cos(2\pi/n))$ is constructible. Thus cos(2π/n) is capable of being constructed, and as a result, a normal n-gon also exists.

Polynomials Belonging To The Galois Group

In order to determine the Galois group that is connected to a polynomial, we need to consider the splitting field that is connected to the polynomial and explore the auto orphisms that are connected to that field. Only then will we be able to determine the Galois group. It is possible to demonstrate that the Galois group is the group that should be considered the corresponding group for these auto orphisms. The calculation of the Galois group of a polynomial may be done in a number of different ways; one example of a typical approach is given below:

1. Start with an equation of the type f(x) for a polynomial over a field F. This equation is often either a rational function or a polynomial with coefficients in F.
2. Determine the field into which the function f(x) divides when applied to the domain F. The splitting field is the smallest field extension of F in which f(x) factors entirely into linear factors. It is also known as the splitting field. In certain circles, it is also referred to as the splitting field.
3. Figure out which of the auto orphisms of the splitting field are responsible for fixing the base field F. When a field isomorphism from the splitting field to itself retains the inverses, addition, and multiplication of the initial field, we refer to this as an auto orphism.

4. Determine the Galois group, which is the group that includes all of the auto orphisms that were found in step 3, since this is the group that encompasses them all. The significance of the group operation may be understood by looking at the composition of auto orphisms.

The Most Important Factor In Dividing The Terms Of An Arithmetic Progression

It is a fact that is well known and not hard to grasp that a product of k consecutive numbers that are bigger than k is divisible by a prime that is greater than k. This fact has become common knowledge throughout the years. It makes no difference whether the numbers go in order or not; this characteristic is always satisfied. The well-known and important theorem of Sylvester states that every product of k consecutive numbers, each of which is bigger than k, must have a prime factor that is greater than k. This theorem states that any product of k consecutive integers must have a prime factor that is higher than k. To put it another way, given positive integers n and k, where n is bigger than k, the following equation is true:

$$P(n(n+1)\cdots(n+k-1)) > k, \quad \text{.....(1)}$$

Let d = 1. As we have shown, P((1, k)) is less than k; hence, the assumption that n is greater than k is required. Schur was the one who rediscovered and supplied more evidence for the result that Sylvester had uncovered, and Erdos offered a further demonstration of the result. For n > k, Moser refined to

$$P(\Delta(n,k)) > \frac{11}{10}k \quad \text{.....(2)}$$

and Hanson made advancements to

$$P(\Delta(n,k)) > 1.5k \quad \text{.....(3)}$$

$$P(\Delta(n,k)) > 2k \quad \text{.....(4)}$$

if the value of n is more than or equal to the least prime that is larger than 2k and (n, k), (8, 2), (8, 3), then the condition is met.

When the value of k is sufficiently high, Ramachandra and Shorey were able to derive more accurate estimations of the parameter P((n, k)) by demonstrating that

$$P(\Delta(n,k)) > c_3 k \log k \left(\frac{\log\log k}{\log\log\log k}\right)^{\frac{1}{2}} \text{ if } n > k^{\frac{3}{2}} \quad \text{.....(5)}$$

where c3 > 0 is a constant that can be computed absolutely. In addition, the results of Jutila and Shorey allow for the following conclusion to be formed, which is

$$P(\Delta(n,k)) > c_4 k \log k \frac{\log\log k}{\log\log\log k} \text{ if } n > k^{\frac{3}{2}} \quad \text{.....(6)}$$

where the absolute positive computable constant c4 is greater than zero. In addition, Langevin demonstrated that for every given $\epsilon > 0$

where c5 is a computable number depending only on k and ϵ. Also, Langevin sharpened to

$$P(\Delta) > k \text{ if } n > k \quad \text{.....(7)}$$

After then, Shorey and Tijdeman offered evidence to show that

$$P(\Delta) > k \text{ unless } (n,d,k) = (2,7,3)$$

The results of Laishram and Shorey, which showed that Hanson and Faulkner's findings needed to be refined, served as a continuation of this trend by proving that this process should continue. Laishram and Shorey's findings proved that Hanson and Faulkner's findings needed to be refined.

$$P(\Delta(n,k)) > 1.85k \text{ for } n > k \quad \text{.....(8)}$$

Unless $(n,k) \in E_0$ where

$$E_0 = \{(8,3),(6,4),(7,4),(15,13),(16,13)\} \cup \{(k+1,k) : k = 3,4,5,8,11,13,14,18,63\}$$

Additionally, by exchanging n > k for requirements that are more stringent, we obtain improved estimations of P(Δ(n, k)) This may be shown by applying the theorem that is presented below.

Fundamentals Of Galois Groups

Our guide for this section is Hadlock, often known as Had78. An explanation of: Consider the possibility that field F is enlarged by field E. We thus proclaim

$$\mathrm{Gal}(E/F) = \{\varphi \in \mathrm{Aut}(E) | \varphi(c) = c \text{ for all } c \in F\} \quad \text{.....(9)}$$

being E over F's Galois group is the goal.

Lemma. There is a field F, and there is an extension of it called E., $r \in E$ Put f in the form of the deg r = n. $(x) \in F[x]$ represent the polynomial that has the lowest value for r over F. Furthermore, in a certain extension L of E, there are exactly n zeros of f(x) that are unique to themselves.

Due to the fact that deg r equals n, deg $f(x) = n.$ According to the definition $f(x)$ by virtue of the fact that over F is irreducible, according to Theorem 2.8.3 $f(x)$ does not include more than one multiple zero. Based on the findings of Theorem 2.12.3, $f(x)$ a linear component of L of E is divided into linear components in certain application. Because of the fact that the severity of the $f(x)$ is n, and taking into argument $f(x)$ contains no more than one zero, $f(x)$ has a total of n different roots in the letter L.

Definition . L has a number of distinct roots. Given that F is a field and that r is an algebraic element in a field extension E, let us assume that F is a field., $f(x) \in F[x]$ represent the polynomial that minimizes the value of r over F, and $r = r_1, r_2, \ldots, r_n$ contain each and every zero of $f(x)$ in any manner extending the letter L of E. $r_1, r_2, \ldots, r_n$ what are the conjugates of the letter r in the language L?.

Lemma. When field F is expanded by field E, the result is: $\varphi \in \mathrm{Gal}(E/F),\ p(x) \in F[x],$ once and for all $a \in E,\ \varphi(p(a)) = p(\varphi(a)).$

Put in the letter p. $(a) = c_0 + c_1 a + \cdots + c_k a^k \text{ for } c_0, c_1, \ldots, c_k \in F$. $\varphi(c_i) = c_i.$ Then

$$\begin{aligned}\varphi(p(a)) &= \varphi(c_0 + c_1 a + \cdots + c_k a^k) \\ &= \varphi(c_0) + \varphi(c_1)\varphi(a) + \cdots + \varphi(c_k)\varphi(a)^k \\ &= c_0 + c_1\varphi(a) + \cdots + c_k\varphi(a)^k \\ &= p(\varphi(a)).\end{aligned}$$

……..(10)

Theorem. It is assumed that E is equal to F(r), where r is an algebraic over F and has conjugates, and that F is a field. $r = r_1, r_2, \ldots, r_n$ an extension L that incorporates E. Following that, for each and every $\varphi \in \mathrm{Gal}(E/F),\ \varphi(r) = r_i$ am of the opinion that for certain 1 $\leq i \leq n.$ And in addition, for each $r_i \in$ There is just one, and it is E.$\varphi \in$ mpliance with Gal (E/F) $\varphi(r) = r_i,$ [Gal (E/F)] is the notation that is used to indicate the number of conjugates of r in E..

Consider the evidence. $\varphi \in$ Both Gal (E/F) and $f(x) \in F[x]$ is the polynomial that yields the lowest value of r over F. From what is stated in Lemma, $0 = \varphi(0) = \varphi(f(r)) = f(\varphi(r)).$ The beginnings of the $f(x)$ The precise conjugates of are included inside L. $r,$ so $\varphi(r) = r_i$ For a time, I have enjoyed that. $1 \leq i \leq n.$

Conceive of the fact that there are two auto orphisms. φ and ψ inside Gal (E/F) encountering the $\varphi(r) = r_i$ and $\psi(r) = r_i$ That appeals to me for a few reasons. $1 \leq i \leq n.$ Since $\varphi, \psi \in$ Gal (E/F), $\varphi(c) = \psi(c) = c$ for all $c \in F$. By assumption, $\varphi(r) = \psi(r)$ Hence, by, $\varphi = \psi.$ Last but not least, the number of conjugates of r in E is equal to the number of Gal(E/F) conjugates since there is a one-to-one connection between the auto orphisms of Gal(E/F) and the conjugates of f r in E.

The statement that |Gal (E/F)| is true if E is any finite extension of F is stated in Corollary $\leq$ [E : F].

The evidence. Let's say that we have n = [E: F], and that E = F(r), where r is an algebraic conjugate over F $r = r_1, r_2, \ldots, r_m$ with an E. We take notice of the fact that $m \leq n$ there are exactly 27 n conjugates of r in some extension L of E. This is the reason why that is the case. In accordance with there is absolutely no other $\varphi \in$ It is possible to map some i to ri using Gal(E/F) in such a manner that $1 \leq i \leq m.$ Gal (E/F) is the result of this. $\leq$ [E : F].

CONCLUSION

When it comes to the calculation of Galois groups, we provide many techniques. There are two numerical approaches, namely, which are the most important contributions. These methods allow for the realistic computation of Galois groups. The first method, known as the Branch Point method, is available without charge and has been included into Macaulay2; it is based on Bertini's monodrama calculations. In addition, we have shown its utility in a wide range of situations, ranging from statistics to kinematics to enumerative geometry. Fibre products are used in the alternate method for the purpose of determining s-transitivity. Because k is less than or equal to 24, and non-alternating, non-symmetric permutation groups are at most five-transitive, this is a helpful information. The computation of Galois groups is possible by the use of homotopy continuation, as shown by these two methods. The study of field expansions, which may be thought of as mathematical frameworks that broaden the number field, is the primary emphasis of the area of mathematics that is known as Galois theory. This topic is a subfield of number theory, which is an overarching field that contains several subfields. It is believed that Évariste Galois, a French mathematician who was active throughout the 19th century and resided in France, was the first person to come up with the concept. Galois theory offers a comprehensive explanation of the connection that holds between the answers to a polynomial equation and the structure of the field extension that is connected to that equation. This explanation is provided in the context of providing an answer to an equation. This comprehension is presented within the framework of an extended field that is associated with the equation.

REFERENCE:

1. Amice, Y. (1975). Les nombres p-adiques, Collection Sup. Le Math´ematicien, *14*, P.U.F.
2. Aschbacher, M., & Guralnick, R. (1982). Solvable generation of groups and Sylow subgroups of the lower central series. *Journal of Algebra*, *77*(1), 189–201. https://doi.org/10.1016/0021-8693(82)90286-1
3. Aschbacher, M., & Guralnick, R. M. (1989). On abelian quotients of primitive groups. *Proceedings of the American Mathematical Society*, *107*(1), 89–95. https://doi.org/10.1090/S0002-9939-1989-0982398-4
4. Babai, L., Cameron, P. J., & P'alfy, P. (2002). On the orders of primitive groups with restricted nonabelian composition factors. *Journal of Algebra*, *79*, 95–113.
5. *Basic algebra*. (1989) (2nd ed.), *II*. Dover Publications, Inc.
6. Caporaso, L., Harris, J., & Mazur, B. (1997). Uniformity of rational points. *Journal of the American Mathematical Society*, *10*(1), 1–35. https://doi.org/10.1090/S0894-0347-97-00195-1
7. Debes, P. (1986). G-fonctions et Th´eor`eme d'irr´eductibilit´e de Hilbert. *Acta Arithmetica*, *47*(4), 371–402. https://doi.org/10.4064/aa-47-4-371-402
8. Dèbes, P. (1992). On the irreducibility of the polynomials P(t m, Y). *Journal of Number Theory*, *42*(2), 141–157. https://doi.org/10.1016/0022-314X(92)90018-K
9. Dèbes, P. (1996). Hilbert subsets and s-integral points. *Manuscripta Mathematica*, *89*(1), 107–137. https://doi.org/10.1007/BF02567509
10. Eichler, M. (1939). Zum Hilbertschen Irreduzibilittssatz. *Mathematische Annalen, Berlin*, *116*(1), 742–748. https://doi.org/10.1007/BF01597387
11. Fried, M. (1974). On Hilbert's irreducibility theorem. *Journal of Number Theory*, *6*(3), 211–231. https://doi.org/10.1016/0022-314X(74)90015-8
12. Fried, M., & Jarden, M. (1986). *Field arithmetic* (1st ed.). Springer Verlag.
13. Arora, S., & Kaur, A. (2024). Role Of Problem-Solving Ability In Promoting Sustainable Development. *Edumania-An International Multidisciplinary Journal*, *02*(02), 158–164. https://doi.org/10.59231/edumania/9044
14. Gallian, J. A. (2010). *Contemporary abstract algebra* (7th ed.). Cole. Cengage Learning.
15. Hadlock, C. R. (1978). *Field theory and its classical problems*. The Mathematical Association of America, Inc.

16. Jacobson, N. (1985). *Basic algebra* (2nd ed.), *I*. Dover Publications, Inc.
17. Munkres, J. R. (1975). *Topology: A first course*. Prentice Hall, Inc.
18. Rudin, W. (1976). *Principles of mathematical analysis* (3rd ed.). McGraw-Hill, Inc.
19. Kumar, S. (2023). Artificial intelligence: learning and creativity. Eduphoria, 01(01), 13–14. https://doi.org/10.59231
20. Saff, E. B., & Snider, A. D. (2003). *Fundamentals of complex analysis with applications to engineering and science* (3rd ed.). Pearson Education, Inc.
21. Strang, G. (2003). *Introduction to linear algebra* (3rd ed.). Wellesley-Cambridge Press.
22. Wilf, H. S. (1994). *Generatingfunctionology* (2nd ed.). Academic Press, Inc.
23. Fatima, I. (2023). Role of Teachers To impart quality education for equitable learning. *Shodh Sari-An International Multidisciplinary Journal*, *02*(03), 462–471. https://doi.org/10.59231/sari7619